The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Carlos Sanchez Valle -- MyNewsGroups	SQL injection vulnerability in tree.php in MyNewsGroups 0.6 allows remote attackers to execute arbitrary SQL commands via the grp_id parameter.	unknown 2006-07-03	7.0	CVE-2006-3346 BUGTRAQ
Crisoft Ricette -- Crisoft Ricette	PHP remote file inclusion vulnerability in recipe/cookbook.php in CrisoftRicette 1.0pre15b allows remote attackers to execute arbitrary PHP code via a URL in the crisoftricette parameter.	unknown 2006-07-03	7.0	CVE-2006-3343 BUGTRAQ
DeltaScripts -- PHP Classifieds	SQL injection vulnerability in search.php in PHP/MySQL Classifieds (PHP Classifieds) allows remote attackers to execute arbitrary SQL commands via the rate parameter.	unknown 2006-06-30	7.0	CVE-2006-3329 BUGTRAQ XF BID SECTRACK
DeltaScripts -- PHP Classifieds	Cross-site scripting (XSS) vulnerability in AddAsset1.php in PHP/MySQL Classifieds (PHP Classifieds) allows remote attackers to execute arbitrary SQL commands via the (1) ProductName ("Title" field), (2) url, and (3) Description parameters, possibly related to issues in add1.php.	unknown 2006-06-30	7.0	CVE-2006-3330 BUGTRAQ BID FRSIRT SECUNIA XF BID SECTRACK
deV!Lz Clanportal -- deV!Lz Clanportal	SQL injection vulnerability in index.php in deV!Lz Clanportal DZCP 1.3.4 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2006-07-01 2006-07-03	7.0	CVE-2006-3347 OTHER-REF BID FRSIRT SECUNIA
Greg Roelofs -- libpng	Buffer overflow in the png_decompress_chunk function in pngrutil.c in libpng before 1.2.12 allows context-dependent attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors related to "chunk error processing," possibly involving the "chunk_name".	unknown 2006-06-30	7.0	CVE-2006-3334 OTHER-REF BID FRSIRT
Microsoft -- Internet Explorer	Heap-based buffer overflow in HTML Help ActiveX control (hhctrl.ocx) in Microsoft Internet Explorer 6.0 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code by repeatedly setting the Image field of an Internet.HHCtrl.1 object to certain values, possibly related to improper escaping and long strings.	unknown 2006-07-06	7.0	CVE-2006-3357 OTHER-REF BID FRSIRT FRSIRT OSVDB SECUNIA
mpg123 -- mpg123	Heap-based buffer overflow in httpdget.c in mpg123 before 0.59s-rll allows remote attackers to execute arbitrary code via a long URL, which is not properly terminated before being used with the strncpy function. NOTE: This appears to be the result of an incomplete patch for CVE-2004-0982.	unknown 2006-07-06	7.0	CVE-2006-3355 OTHER-REF GENTOO SECUNIA
MyAds -- MyAds	SQL injection vulnerability in annonces-p-f.php in MyAds module 2.04jp for Xoops allows remote attackers to execute arbitrary SQL commands via the lid parameter.	2006-06-28 2006-07-03	7.0	CVE-2006-3341 OTHER-REF BID FRSIRT SECUNIA XF

newsPHP -- newsPHP	Multiple cross-site scripting (XSS) vulnerabilities in index.php in NewsPHP 2006 PRO allow remote attackers to inject arbitrary web script or HTML via the (1) words, (2) id, (3) cat_id, and (4) tim parameters, which are not sanitized before being returned in an error page. NOTE: it is possible that some of these vectors are resultant from an SQL injection issue.	2006-06-29 2006-07-06	7.0	CVE-2006-3358 BUGTRAQ FRSIRT SECUNIA
newsPHP -- newsPHP	Multiple SQL injection vulnerabilities in index.php in NewsPHP 2006 PRO allow remote attackers to inject arbitrary web script or HTML via the (1) words, (2) id, (3) topmenuitem, and (4) cat_id parameters in (a) index.php; and the (5) category parameter in (b) inc/rss_feed.php.	2006-06-29 2006-07-06	7.0	CVE-2006-3359 BUGTRAQ
PHPOutsourcing -- Zorum	SQL injection vulnerability in index.php in Zorum Forum 3.5 allows remote attackers to execute arbitrary SQL commands via the (1) offset, (2) tid, (3) fromid, (4) sortby, (5) fromfrommethod, and (6) fromfromlist parameters.	unknown 2006-06-30	7.0	CVE-2006-3332 OTHER-REF BID SECTRACK
Randshop -- Randshop	PHP remote file inclusion vulnerability in index.php in Randshop 1.2 and earlier, including 0.9.3, allows remote attackers to execute arbitrary PHP code via a URL in the incl parameter.	unknown 2006-07-06	7.0	CVE-2006-3374 BUGTRAQ BUGTRAQ BID
Randshop -- Randshop	PHP remote file inclusion vulnerability in includes/header.inc.php in Randshop 1.1.1 allows remote attackers to execute arbitrary PHP code via the dateiPfad parameter.	unknown 2006-07-06	7.0	CVE-2006-3375 OTHER-REF BID
Samba -- ppp	The winbind plugin in pppd for ppp 2.4.4 and earlier does not check the return code from the setuid function call, which might allow local users to gain privileges by causing setuid to fail, such as exceeding PAM limits for the maximum number of user processes, which prevents the winbind NTLM authentication helper from dropping privileges.	unknown 2006-07-05	7.0	CVE-2006-2194 UBUNTU
SmS Script -- SmS Script	Multiple SQL injection vulnerabilities in SmS Script allow remote attackers to execute arbitrary SQL commands via the CatID parameter in (1) cat.php and (2) add.php.	unknown 2006-07-03	7.0	CVE-2006-3349 BUGTRAQ
SWsoft -- HSPcomplete	Multiple SQL injection vulnerabilities in HSPcomplete 3.2.2 and 3.3 Beta and earlier allow remote attackers to execute arbitrary SQL commands via the (1) type parameter in report.php and (2) level parameter in custom_buttons.php.	unknown 2006-07-03	7.0	CVE-2006-3348 OTHER-REF
Ubuntu -- Ubuntu Linux	passwd command in shadow in Ubuntu 5.04 through 6.06 LTS, when called with the -f, -g, or -s flag, does not check the return code of a setuid call, which might allow local users to gain root privileges if setuid fails in cases such as PAM failures or resource limits.	unknown 2006-07-06	7.0	CVE-2006-3378 UBUNTU
wvWare -- wv2 wvWare -- libwmf	Integer overflow in player.c in libwmf 0.2.8.4, as used in multiple products including (1) wv, (2) abiword, (3) freetype, (4) gimp, (5) libgsf, and (6) imagemagick allows remote attackers to execute arbitrary code via the MaxRecordSize header field in a WMF file.	unknown 2006-07-06	7.0	CVE-2006-3376 BUGTRAQ BID FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
BLOG:CMS -- BLOG:CMS	SQL injection vulnerability in index.php in the NP_SEO plugin in BLOG:CMS before 4.1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2006-07-06	4.7	CVE-2006-3364 BUGTRAQ OTHER-REF OTHER-REF FRSIRT OSVDB SECTRACK SECUNIA XF
COWON America -- jetAudio	Buffer overflow in jetAudio 6.2.6.8330 (Basic), and possibly other versions, allows user-complicit attackers to execute arbitrary code via an audio file (such as WMA) with long ID Tag values including (1) Title, (2) Author, and (3) Album, which triggers the overflow in the tooltip display string if the sound card driver is disabled or incorrectly installed.	unknown 2006-07-05	4.7	CVE-2006-2910 OTHER-REF BID FRSIRT SECUNIA
Fusionphp -- Fusion News	Directory traversal vulnerability in sources/post.php in Fusion News 1.0, when register_globals is enabled, allows remote attackers to include arbitrary files via a .. (dot dot) sequence in the fil_config parameter, which can be used to execute PHP code that has been injected into a log file.	unknown 2006-07-06	4.7	CVE-2006-3387 OTHER-REF XF
Geeklog -- Geeklog	connectors/php/connector.php in FCKeditor mcpuk file manager in Geeklog 1.4.0 through 1.4.0sr3, when installed on Apache with mod_mime, allows remote attackers to execute arbitrary PHP code by uploading and accessing a	unknown 2006-07-06	5.6	CVE-2006-3362 OTHER-REF OTHER-REF

	.php file that ends in an allowed extension.			OTHER-REF BID FRSIRT SECUNIA XF
HP -- HP-UX	Unspecified vulnerability in mkdir in HP-UX B.11.00, B.11.04, B.11.11, and B.11.23 allows local users to gain privileges via unknown attack vectors.	unknown 2006-07-02	4.9	CVE-2006-3335 HP BID FRSIRT SECTRACK
iMBC -- iMBCContents ActiveX Control	The Execute function in iMBCContents ActiveX Control before 2.0.0.59 allows remote attackers to execute arbitrary files via the file URI handler.	unknown 2006-07-06	4.7	CVE-2006-3391 FRSIRT SECUNIA
mAds -- mAds	Cross-site scripting (XSS) vulnerability in index.php in mAds 1.0 allows remote attackers to inject arbitrary web script or HTML via Javascript events such as onmouseover within a URL. NOTE: the provenance of this information is unknown; the details are obtained solely from third party reports.	unknown 2006-07-06	4.7	CVE-2006-3383 FRSIRT SECUNIA
Mozilla -- Firefox	** DISPUTED ** Cross-domain vulnerability in Mozilla Firefox allows remote attackers to access restricted information from other domains via an object tag with a data parameter that references a link on the attacker's originating site that specifies a Location HTTP header that references the target site, which then makes that content available through the outerHTML attribute of the object. NOTE: this description was based on a report that has since been retracted by the original authors. The authors misinterpreted their test results. Other third parties also disputed the original report. Therefore, this is not a vulnerability. It is being assigned a candidate number to provide a clear indication of its status.	unknown 2006-07-05	4.7	CVE-2006-3352 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ OTHER-REF BID
pearlinger -- Pearl for Mambo	Multiple PHP remote file inclusion vulnerabilities in Pearl For Mambo module 1.6 for Mambo, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via the (1) phpbb_root_path parameter in (a) includes/functions_cms.php and the (2) GlobalSettings[templatesDirectory] parameter in multiple files in the "includes" directory including (b) adminSensored.php, (c) adminBoards.php, (d) adminAttachments.php, (e) adminAvatars.php, (f) adminBackupdatabase.php, (g) adminBanned.php, (h) adminForums.php, (i) adminPolls.php, (j) adminSmileys.php, (k) poll.php, and (l) move.php.	2006-06-27 2006-07-03	5.6	CVE-2006-3340 OTHER-REF BID FRSIRT SECUNIA
phpMyAdmin -- phpMyAdmin	Cross-site scripting (XSS) vulnerability in phpMyAdmin before 2.8.2 allows remote attackers to inject arbitrary web script or HTML via the table parameter.	unknown 2006-07-06	4.7	CVE-2006-3388 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Siemens -- Speedstream Wireless Router	Siemens Speedstream Wireless Router 2624 allows local users to bypass authentication and access protected files by using the UPnP (Universal Plug and Play)/1.0 component.	2006-05-02 2006-07-03	4.9	CVE-2006-3344 BUGTRAQ OTHER-REF FRSIRT SECUNIA
SpiffyJr -- phpRaid	SQL injection vulnerability in includes/functions_logging.php in phpRaid 3.0.5, and possibly other versions, allows remote attackers to execute arbitrary SQL commands via the log_hack function.	unknown 2006-06-30	5.6	CVE-2006-3322 OTHER-REF SECUNIA XF BUGTRAQ BID FRSIRT
Stud.IP -- Stud.IP	PHP remote file inclusion vulnerability in Stud.IP 1.3.0-2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the (1) _PHPLIB[libdir] parameter in studip-phplib/oohforms.inc and (2) ABSOLUTE_PATH_STUDIP parameter in studip-htdocs/archiv_assi.php.	unknown 2006-07-06	5.6	CVE-2006-3361 OTHER-REF FRSIRT SECTRACK XF
Sun -- StarOffice OpenOffice -- OpenOffice	OpenOffice.org (aka StarOffice) 1.1.x up to 1.1.5 and 2.0.x before 2.0.3 allows user-complicit attackers to conduct unauthorized activities via an OpenOffice document with a malicious BASIC macro, which is executed without prompting the user.	unknown 2006-06-30	5.6	CVE-2006-2198 OTHER-REF SUNALERT
Sun -- StarOffice OpenOffice -- OpenOffice	Heap-based buffer overflow in OpenOffice.org (aka StarOffice) 1.1.x up to 1.1.5 and 2.0.x before 2.0.3 allows user-complicit attackers to execute arbitrary code via a crafted OpenOffice XML document that is not properly handled by (1) Calc, (2) Draw, (3) Impress, (4) Math, or (5) Writer, aka "File Format / Buffer Overflow Vulnerability."	unknown 2006-06-30	5.6	CVE-2006-3117 OTHER-REF OTHER-REF SUNALERT OTHER-REF

TWiki -- TWiki	TWiki 01-Dec-2000 up to 4.0.3 allows remote attackers to bypass the upload filter and execute arbitrary code via filenames with double extensions such as ".php.en", ".php.1", and other allowed extensions that are not .txt. NOTE: this is only a vulnerability when the server allows script execution in the pub directory.	unknown 2006-07-05	4.7	CVE-2006-3336 OTHER-REF FRSIRT
Vincent Leclercq -- Vincent Leclercq News	SQL injection vulnerability in divers.php in Vincent Leclercq News 5.2 allows remote attackers to execute arbitrary SQL commands via the (1) id and (2) texte parameters.	unknown 2006-07-06	4.7	CVE-2006-3384 OTHER-REF BID FRSIRT SECUNIA
Vincent Leclercq -- Vincent Leclercq News	Cross-site scripting (XSS) vulnerability in divers.php in Vincent Leclercq News 5.2 allows remote attackers to inject arbitrary web script or HTML via the (1) id and (2) disabled parameters.	unknown 2006-07-06	4.7	CVE-2006-3385 OTHER-REF BID FRSIRT SECUNIA
Xoops -- Xoops Glossaire Module	PHP remote file inclusion vulnerability in index.php in the Glossaire module 1.7 for Xoops allows remote attackers to execute arbitrary PHP code via a URL in the pa parameter.	unknown 2006-07-06	5.6	CVE-2006-3363 BUGTRAQ BID SECTRACK

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Ajax Softwares -- AliPAGER	Cross-site scripting (XSS) vulnerability in AliPAGER, possibly 1.5 and earlier, allows remote attackers to inject arbitrary web script or HTML via a chat line.	unknown 2006-07-03	2.3	CVE-2006-3345 BUGTRAQ
Apple -- Mac OS X Server Apple -- Mac OS X	The TIFFFetchAnyArray function in ImageIO in Apple OS X 10.4.7 and earlier allows remote user-complicit attackers to cause a denial of service (application crash) via an invalid tag value in a TIFF image, possibly triggering a null dereference. NOTE: This is a different issue than CVE-2006-1469.	2006-05-15 2006-07-06	1.9	CVE-2006-3356 OTHER-REF FRSIRT XF
Apple -- Safari	Apple Safari 2.0.4/419.3 allows remote attackers to cause a denial of service (application crash) via a DHTML setAttributeNode function call with zero arguments, which triggers a null dereference.	unknown 2006-07-06	2.3	CVE-2006-3372 OTHER-REF BID FRSIRT OSVDB
Atlassian -- JIRA	Cross-site scripting (XSS) vulnerability in Atlassian JIRA 3.6.2-#156 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors in a direct request to secure/ConfigureReleaseNote.jspa, which are not sanitized before being returned in an error page.	unknown 2006-07-03	1.9	CVE-2006-3338 OTHER-REF FRSIRT
Atlassian -- JIRA	secure/ConfigureReleaseNote.jspa in Atlassian JIRA 3.6.2-#156 allows remote attackers to obtain sensitive information via unspecified manipulations of the projectId parameter, which displays the installation path and other system information in an error message.	unknown 2006-07-03	2.3	CVE-2006-3339 OTHER-REF FRSIRT
bb-news -- Blueboy	Blueboy 1.0.3 stores bb_news_config.inc under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information, including the database configuration.	unknown 2006-07-06	2.3	CVE-2006-3370 BUGTRAQ
cPanel -- cPanel	Cross-site scripting (XSS) vulnerability in frontend/x/files/select.html in cPanel 10.8.2-CURRENT 118 and earlier allows remote attackers to inject arbitrary web script or HTML via the file parameter.	2006-06-09 2006-07-03	1.9	CVE-2006-3337 BUGTRAQ BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA
Efone -- Efone	Efone 20000723 stores config.inc under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information.	unknown 2006-07-06	2.3	CVE-2006-3368 BUGTRAQ BID FRSIRT SECUNIA
Eupla -- Foros	Eupla Foros 1.0 stores the inc/config.inc file under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information, including the database configuration.	unknown 2006-07-06	2.3	CVE-2006-3371 BUGTRAQ BID FRSIRT SECUNIA
FreeStyle Wiki -- FreeStyle Wiki	Algorithmic complexity vulnerability in FreeStyle Wiki before 3.6.2 allows remote attackers to cause a denial of service (CPU consumption) by performing a diff between large, crafted pages that trigger the worst case.	unknown 2006-07-06	2.3	CVE-2006-3380 OTHER-REF OTHER-REF

				FRSIRT SECUNIA
Hiki -- Hiki	Algorithmic complexity vulnerability in Hiki Wiki 0.6.0 through 0.6.5 and 0.8.0 through 0.8.5 allows remote attackers to cause a denial of service (CPU consumption) by performing a diff between large, crafted pages that trigger the worst case.	unknown 2006-07-06	3.3	CVE-2006-3379 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Hobbit Monitor -- Hobbit Monitor	Unspecified vulnerability in the client/bin/logfetch script in Hobbit 4.2-beta allows local users to read arbitrary files, related to logfetch running as setuid root.	unknown 2006-07-06	1.6	CVE-2006-3373 BUGTRAQ BID
Iduprey -- Kamikaze-QSCM	Kamikaze-QSCM 0.1 stores config.inc under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information, including the database configuration.	unknown 2006-07-06	2.3	CVE-2006-3369 BUGTRAQ BID FRSIRT SECUNIA
JMB Software -- AutoRank	Cross-site scripting (XSS) vulnerability in JMB Software AutoRank PHP 3.02 and earlier, and AutoRank Pro 5.01 and earlier, allows remote attackers to inject arbitrary web script or HTML via the (1) Keyword parameter in search.php and the (2) Username parameter in main.cgi.	2006-06-25 2006-07-06	3.7	CVE-2006-3377 OTHER-REF FRSIRT SECTRACK SECTRACK SECUNIA
Linux -- Linux kernel	The dvd_read_bca function in the DVD handling code in drivers/cdrom/cdrom.c in Linux kernel 2.2.16, and later versions, assigns the wrong value to a length variable, which allows local users to execute arbitrary code via a crafted USB Storage device that triggers a buffer overflow.	unknown 2006-07-05	3.3	CVE-2006-2935 OTHER-REF
mAds -- mAds	Cross-site scripting (XSS) vulnerability in search.php in mAds 1.0 allows remote attackers to inject arbitrary web script or HTML via the "search string".	unknown 2006-07-06	2.3	CVE-2006-3382 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Microsoft -- Windows Server 2003 Microsoft -- Windows XP	Buffer overflow in Windows Explorer (explorer.exe) on Windows XP and 2003 allows user-complicit attackers to cause a denial of service (repeated crash) and possibly execute arbitrary code via a .url file with an InternetShortcut tag containing a long URL and a large number of "file:" specifiers.	unknown 2006-07-05	1.9	CVE-2006-3351 BUGTRAQ
Microsoft -- Internet Explorer	Microsoft Internet Explorer 6 allows remote attackers to cause a denial of service (crash) by setting the Filter property of an ADODB.Recordset ActiveX object to certain values multiple times, which triggers a null dereference.	unknown 2006-07-05	2.3	CVE-2006-3354 OTHER-REF BID OSVDB
Mp3NetBox -- Mp3NetBox	Mp3 JudeBox Server (Mp3NetBox) Beta 1 stores config.inc under the web document root with insufficient access control, which allows remote attackers to obtain sensitive information, including the database configuration.	unknown 2006-07-06	2.3	CVE-2006-3367 BUGTRAQ
Olate -- Arctic	Cross-site scripting (XSS) vulnerability in index.php in Arctic 1.0.2 and earlier allows remote attackers to inject arbitrary web script or HTML via the query parameter in a search cmd.	unknown 2006-07-03	1.9	CVE-2006-3342 OTHER-REF OTHER-REF OSVDB SECUNIA
Opera Software -- Opera Web Browser	Opera before 9.0 does not reset the SSL security bar after displaying a download dialog from an SSL-enabled website, which allows remote attackers to spoof a trusted SSL certificate from an untrusted website and facilitates phishing attacks.	unknown 2006-06-30	2.3	CVE-2006-3331 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA XF
Opera Software -- Opera Web Browser	Opera 9 allows remote attackers to cause a denial of service (crash) via a crafted web page that triggers an out-of-bounds memory access, related to an iframe and javascript that accesses certain style sheets properties.	unknown 2006-07-05	2.3	CVE-2006-3353 BUGTRAQ OTHER-REF BID XF
PHPOutsourcing -- Zorum	Cross-site scripting (XSS) vulnerability in index.php in Zorum Forum 3.5 allows remote attackers to inject web script or HTML via the multiple unspecified parameters, including the (1) frommethod, (2) list, and (3) method, which are reflected in an error message. NOTE: some of these vectors might be resultant from SQL injection.	unknown 2006-06-30	1.9	CVE-2006-3333 OTHER-REF

phpSysInfo -- phpSysInfo	Directory traversal vulnerability in index.php in phpSysInfo 2.5.1 allows remote attackers to determine the existence of arbitrary files via a .. (dot dot) sequence and a trailing null (%00) byte in the lng parameter, which will display a different error message if the file exists.	unknown 2006-07-06	2.3	CVE-2006-3360 FULLDISC FULLDISC FRSIRT SECUNIA
SturGeoN Upload -- SturGeoN Upload	SturGeoN Upload allows remote attackers to execute arbitrary PHP code by uploading a file with a .php extension, then directly accessing the file. NOTE: It is uncertain whether this is a vulnerability or a feature of the product.	unknown 2006-07-06	2.3	CVE-2006-3381 BUGTRAQ OTHER-REF BID
Sun -- StarOffice OpenOffice -- OpenOffice	Unspecified vulnerability in Java Applets in OpenOffice.org 1.1.x (aka StarOffice) up to 1.1.5 and 2.0.x before 2.0.3 allows user-complicit attackers to escape the Java sandbox and conduct unauthorized activities via certain applets in OpenOffice documents.	unknown 2006-06-30	3.7	CVE-2006-2199 OTHER-REF SUNALERT
V3 Chat -- V3 Chat	mail/index.php in V3 Chat allows remote attackers to obtain the installation path via the id parameter, which displays the path in an error page due to an incorrect SQL statement.	unknown 2006-07-06	1.9	CVE-2006-3365 BUGTRAQ BUGTRAQ SECTRACK
V3 Chat -- V3 Chat	Multiple cross-site scripting (XSS) vulnerabilities in V3 Chat allow remote attackers to inject arbitrary web script or HTML via crafted HTML tags, as demonstrated by the IMG tag, in the (1) id parameter in (a) mail/index.php and (b) mail/reply.php; (2) login_id parameter in (c) members/is_online.php; (3) site_id parameter in (d) messenger/online.php, (e) messenger/search.php, and (f) messenger/profile.php; (4) contact_name parameter in messenger/search.php; (5) membername parameter in (g) messenger/profileview.php; (6) unspecified parameters used when "editing a profile"; and (7) cust_name parameter in (h) messenger/expire.php. NOTE: The vendor disputes the vectors involving files in the messenger directory, stating "... the referenced folder 'messenger' was never available to the general public...".	unknown 2006-07-06	1.9	CVE-2006-3366 BUGTRAQ BUGTRAQ SECTRACK
Vincent Leclercq -- News	index.php in Vincent Leclercq News 5.2 allows remote attackers to obtain sensitive information, such as the installation path, via a mail[] parameter with invalid values.	unknown 2006-07-06	2.3	CVE-2006-3386 OTHER-REF SECUNIA
WordPress -- WordPress	index.php in WordPress 2.0.3 allows remote attackers to obtain sensitive information, such as SQL table prefixes, via an invalid paged parameter, which displays the information in an SQL error message. NOTE: this issue has been disputed by a third party who states that the issue does not leak any target-specific information.	unknown 2006-07-06	2.3	CVE-2006-3389 BUGTRAQ BUGTRAQ BUGTRAQ BID FRSIRT SECUNIA
WordPress -- WordPress	WordPress 2.0.3 allows remote attackers to obtain the installation path via a direct request to various files, such as those in the (1) wp-admin, (2) wp-content, and (3) wp-includes directories, possibly due to uninitialized variables.	unknown 2006-07-06	2.3	CVE-2006-3390 BUGTRAQ BUGTRAQ BID FRSIRT SECUNIA

Back to top

Last updated July 10, 2006